

## IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

### Listing of Claims:

1. (Currently Amended) A method of providing security, comprising:

accessing a prefetch file configured to store operational information comprising an identification of one or more resources accessed by a process during initialization of the process, which prefetch file an operating system with which the process is associated, or a component or module of the operating system, is configured to use in the event of a subsequent initialization of the process to prefetch at least one of said one or more resources prior to access to said at least one of said one or more resources being requested by the process;

determining a first behavior using the operational information, wherein the first behavior is associated with the process;

monitoring the process; comparing a second behavior with the first behavior, wherein the second behavior is attempted by the process; and

performing a predetermined responsive action if the second behavior is different from the first behavior;

wherein determining the first behavior includes parsing the prefetch file to identify the one or more resources and wherein the second behavior is determined to be different from the first behavior if the second behavior comprises an attempt by the process to access a resource not included in the one or more resources; and

further comprising monitoring the prefetch file for changes to the prefetch file and in the event a change to the prefetch file is detected reparsing the prefetch file to determine whether any new resource in addition to the one or more resources is included in the prefetch file as changed and, in the event any such new resource is included in the prefetch file as changed determining a third behavior associated with the process, which

third behavior comprises accessing said new resource and which third behavior is considered to be an authorized behavior of the process.

2. (Previously Presented) The method of providing security as recited in Claim 1, in an event the second behavior is determined to be different from the first behavior, the second behavior is determined to be disallowed.
3. (Previously Presented) The method of providing security as recited in Claim 1, wherein the first behavior is one of a plurality of behaviors determined using the operational information.
4. (Previously Presented) The method of providing security as recited in Claim 1, wherein the first behavior is one of a plurality of behaviors determined using the operational information, and in the event the second behavior is determined to be different from the plurality of behaviors, the second behavior is determined to be disallowed.
5. (Previously Presented) The method of providing security as recited in Claim 1, further comprising determining that the second behavior is disallowed.
6. (Previously Presented) The method of providing security as recited in Claim 1, further comprising determining that the second behavior is disallowed and performing a predetermined action.
7. (Previously Presented) The method of providing security as recited in Claim 1, wherein the predetermined action includes preventing the second behavior from succeeding.
8. (Previously Presented) The method of providing security as recited in Claim 1, wherein the predetermined action includes generating an event associated with the second behavior.
9. (Previously Presented) The method of providing security as recited in Claim 1, wherein determining the first behavior using the operational information is performed when the process is not operating.
10. (Canceled)

11. (Previously Presented) The method of providing security as recited in Claim 1, wherein the operational information includes information is used to improve process initialization time.
12. (Previously Presented) The method of providing security as recited in Claim 1, wherein the operational information is configured on a per user basis.
13. (Previously Presented) The method of providing security as recited in Claim 1, wherein the operational information includes component access information.
14. (Canceled)
15. (Previously Presented) The method of providing security as recited in Claim 1, wherein the file includes a superfetch file.
16. (Currently Amended) A system for providing security, comprising:

a processor configured to:

access a prefetch file configured to store operational information comprising an identification of one or more resources accessed by a process during initialization of the process, which prefetch file an operating system with which the process is associated, or a component or module of the operating system, is configured to use in the event of a subsequent initialization of the process to prefetch at least one of said one or more resources prior to access to said at least one of said one or more resources being requested by the process;

determine a first behavior using the operational information, wherein the first behavior is associated with the process;

monitor the process;

compare a second behavior with the first behavior, wherein the second behavior is attempted by the process; and

perform a predetermined responsive action if the second behavior is different from the first behavior; and

a memory coupled with the processor, configured to provide the processor with directions;

wherein determining the first behavior includes parsing the prefetch file to identify the one or more resources and wherein the second behavior is determined to be

different from the first behavior if the second behavior comprises an attempt by the process to access a resource not included in the one or more resources; and

wherein the processor is further configured to monitor the prefetch file for changes to the prefetch file and in the event a change to the prefetch file is detected reparse the prefetch file to determine whether any new resource in addition to the one or more resources is included in the prefetch file as changed and, in the event any such new resource is included in the prefetch file as changed to determine a third behavior associated with the process, which third behavior comprises accessing said new resource and which third behavior is considered to be an authorized behavior of the process.

17. (Currently Amended) A computer program product for providing security, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

accessing a prefetch file configured to store operational information comprising an identification of one or more resources accessed by a process during initialization of the process, which prefetch file an operating system with which the process is associated, or a component or module of the operating system, is configured to use in the event of a subsequent initialization of the process to prefetch at least one of said one or more resources prior to access to said at least one of said one or more resources being requested by the process;

determining a first behavior using the operational information, wherein the first behavior is associated with the process;

monitoring the process;

comparing a second behavior with the first behavior, wherein the second behavior is attempted by the process; and

performing a predetermined responsive action if the second behavior is different from the first behavior;

wherein determining the first behavior includes parsing the prefetch file to identify the one or more resources and wherein the second behavior is determined to be different from the first behavior if the second behavior comprises an attempt by the process to access a resource not included in the one or more resources; and

further comprising computer instructions for monitoring the prefetch file for changes to the prefetch file and in the event a change to the prefetch file is detected reparsing the prefetch file to determine whether any new resource in addition to the one or more resources is included in the prefetch file as changed and, in the event any such new resource is included in the prefetch file as changed determining a third behavior associated with the process, which third behavior comprises accessing said new resource and which third behavior is considered to be an authorized behavior of the process.

18. (Canceled)
19. (Canceled)
20. (Canceled)